

INSAI

SPECIFICATIONMETHOD AND COMMUNICATIONS SYSTEM FOR CIPHERINGINFORMATION FOR A RADIO TRANSMISSION AND FORAUTHENTICATING OF SUBSCRIBERS

5 The invention is directed to a method for the encryption of information for a radio transmission and for authentication of subscribers in a communication system and is also directed to a corresponding communication system.

*Description of the related Art*

10 Communication systems such as, ~~for example,~~ the mobile radio telephone system according to the GSM standard (global system for mobile communication) use a radio interface for wireless information transmission.

*Connection*  
*connections* between mobile stations and base stations of a mobile radio telephone network *can be* being capable of being setup, released and maintained on *this* radio interface. A method and a system for encryption (ciphering)

15 information for radio transmission and for subscriber authentication are known from the article "Safety First bei europaweiter Mobilkommunikation", telcom report 16 (1993), No. 6, pages 326 through 329. *in this article, the* The mobile

subscribers ~~thereby~~ identify themselves with respect to the mobile radio telephone network using a ~~means - also referred to as~~ subscriber identity

20 mobile ~~or~~ (SIM) card that is contained in the radio telephone subscriber station. At the network side, the mobile subscriber is registered in a ~~means -~~

~~for example,~~ an authentication means (authentication center) that respectively offers security parameters and security algorithms for the

25 protection of the subscriber data of the mobile subscribers. The encryption of the information on the radio interface *takes place in a* ensures subscriber-related *manner* and is

directly coupled to the subscriber authentication.

In future communication systems, such as, ~~for example,~~ a universal network (UMTS, universal mobile telecommunication system or UPT,

30 universal personal communication), there is *the* tendency to divide the infrastructure into an access network and into one or more core networks.

*in these systems*  
 The area of the access network ~~is thereby~~ responsible for matters of the radio interface such as administration and allocation of the radio channels, channel encoding, encryption via the radio interface, ~~etc., in contrast~~ *By contrast,* where the area of the core network is mainly responsible for matters of the subscriber administration such as registration (subscription), authentication, selection of the access network, etc., as well as for offering services. An encryption of the information for the radio transmission independently of the core network is impossible in the current GSM system. Over and above this, a radio resource, for example the radio channel, is exclusively used for only one subscriber in the encryption, namely the subscriber that was authenticated at the moment ~~this no longer being adequate~~ *This is for* in future communication systems, particularly given simultaneous use of a mobile station by a plurality of subscribers (for example, with their SIM cards).

*Ins 5 a 2*  
 The invention is based on the object of specifying a method and a communication system that enables an encryption of the information at the radio interface independently of the nature and plurality of core networks, ~~so~~ *enabling* that a functional separation of encryption and authentication ~~derives~~.

*Ins 5 a 3* ~~This object is inventively achieved by the method comprising the features of patent claim 1 and by the communication system comprising the features of patent claim 12. Developments of the invention can be derived from the subclaims.~~

The subject matter of the invention proceeds from an encryption of the information for the radio transmission in an access network as well as from an authentication in at least one core network. Inventively, public keys are transmitted in alternation between a mobile station that can be used in parallel by a plurality of subscribers and the base station, being sent via the radio interface, and the public key received by the base station or ~~the~~ *the* respectively, mobile station is employed for the encryption of the information to be subsequently transmitted via the radio interface. The encrypted information received by the mobile station or ~~the~~ *the* respectively, base station can be deciphered on the basis of a private key that is allocated in the mobile station or ~~the~~ *the* respectively, in the base station to the public key that was

transmitted. Following the deciphering procedure, the authentication of the  
 respective core network is implemented by a <sup>component/equipment</sup> means of the mobile station,  
 and the authentication of the subscriber is implemented by <sup>a component/equipment</sup> the means of the  
 core network on the basis of the encrypted information transmitted in  
 alternation.

As a result of the mutual transmission of public keys between mobile  
 station and base station, the encryption for the radio transmission can <sup>take place in</sup> ~~ensue~~  
 mobile station-related <sup>manner</sup> instead of <sup>a</sup> subscriber-related <sup>manner</sup> and, thus, can  
 simultaneously ensue for a plurality of subscribers. There is a bidirectional,  
 trusted relationship into which an "apparent" base station or an unauthorized  
 base station cannot intervene. Another advantage is the functional  
 separation of access network <sup>(responsible for encryption)</sup> and core  
 network <sup>(responsible for authentication)</sup>. The radio resource is multiply  
 utilized for the encryption of a plurality of subscribers at the mobile station.  
 The information required for the authentication procedure can already be  
 transmitted encrypted, <sup>which was not</sup> ~~this having not been~~ possible in the previous GSM  
 system. Maximum security is achieved by the combination of the encryption  
 with public/private keys at the mobile station level and the following  
 authentication at the subscriber level. In particular, a plurality of core  
 networks - potentially of different network types - can be connected parallel  
 to the access network due to the functional separation of access network  
 and core network, and, in particular, a plurality of subscribers having  
 different identities (SIM cards) can communicate simultaneously via a mobile  
 station and in different core networks.

No third party can subsequently sneak into the secure connection,  
 achieved by multiple, mutual transmission of the public keys. The following  
 authentication assures that the respective partner <sup>device</sup> ~~means~~ of the connection -  
 i.e., the base station from the point of view of the mobile station or,  
 respectively, the mobile station from the point of view of the base station -  
 is also in fact the <sup>device</sup> ~~means~~ that it pretended to be at the beginning of the  
 communication.

An advantageous development of the invention provides that the mobile station first sends a first public key to the base station, ~~that latter~~ *which uses this key* using this for the encryption of the information, and a public key is sent from the base station to the mobile station that employs it for the encryption of the information. Subsequently, the mobile station sends a second public key to the base station. The involvement of an "apparent" base station or of the unauthorized base station into the connection is thus dependably prevented at the radio interface. The second key thereby preferably replaces the first key.

According to an alternative development of the invention, the base station first sends a first public key to the mobile station, which employs it for encryption of the information, and the mobile station sends a public key to the base station, which employs it for the encryption of the information. Subsequently, the base station sends a second public key to the mobile station. The involvement of the "apparent" base station or of the unauthorized base station in the connection is thus dependably prevented at the radio interface. The second key is thereby preferably replaced by the first key.

It is advantageous according to another development of the invention that the mobile station sends a subscriber identity of the subscriber and an authentication request to the core network in encrypted form and receives an authentication reply from the ~~means of the~~ core network sent back to it in encrypted form. Subsequently, the mobile station implements an authentication procedure for checking the identity of the core network. A network authentication thus *occurs* ~~ensues~~ at the side of the mobile station, *which can be* ~~this~~ *being capable of being* individually implemented, particularly *for* a plurality of core networks dependent on where the subscriber is registered.

The ~~means of the~~ core network preferably sends an authentication request in addition to the authentication reply in encrypted fashion, and an authentication reply is sent back to the ~~means from the~~ mobile station in encrypted form. Subsequently, ~~the means of~~ the core network can implement an authentication procedure for checking the subscriber identity.

This has the advantage that the request for checking the subscriber authentication can be co-transmitted with the reply of the network <sup>core</sup> means to the network authentication and can be initiated by the network <sup>core</sup> means immediately upon arrival of the reply.

5 A communication system according to the invention comprises memory ~~means~~ as a mobile station that can be used in parallel by a plurality of subscribers and of the base station for storing public keys and private keys that are allocated to the public keys. Transmission devices in the mobile station and in the base station <sup>implement</sup> see to the mutual transmission of the public keys via the radio interface. Control devices in the mobile station and in the base station are provided for the encryption of the information to be subsequently transmitted via the radio interface upon employment of the public key received from the base station or, ~~respectively~~, mobile station and for deciphering the received, encrypted information on the basis of the stored, appertaining private key. Over and above this, the communication system comprises a subscriber-specific <sup>authentication mechanism</sup> ~~means~~ in the mobile station and a <sup>controller</sup> ~~control means~~ in the respective core network for the implementation of the authentication of the core network as well as of the authentication of the subscribers on the basis of mutually transmitted, encrypted information.

20 <sup>In 5a47</sup> The invention is explained in greater detail below on the basis of an exemplary embodiment with reference to the graphic illustration.

~~Thereby shown are:~~

- FIG. 1 <sup>is a</sup> ~~the~~ block circuit diagram of a communication system with an access network for the radio transmission and a plurality of core networks for the authentication;
- 25 FIG. 2 <sup>is a</sup> ~~the~~ message flow <sup>diagram</sup> for the encryption of the information at the radio interface between a mobile station and a base station of the access network; and
- FIG. 3 <sup>is a</sup> ~~the~~ message flow <sup>diagram</sup> for the authentication of the subscribers and of the core networks between the mobile station and a ~~network~~ <sup>means</sup> of the respective core network.
- 30

Ins 257

universal

The communication system show in FIG. 1 is a communication system UNW - such as, ~~for example~~, a universal UMTS or UPT network (universal mobile telecommunication system or universal personal telecommunication) - whose infrastructure is divided into an access network ACN and into one or more core networks CON1, CON2. The area of the access network ACN having devices of a radio sub-system - such as, ~~for example~~, base stations BS and base station controllers BSC connected ~~thereto~~ <sup>to it - is</sup> ~~thereby~~ responsible for matters of the radio interface such as administration and allocation of radio channels, channel encoding, encryption via the radio interface, etc. The area of the core network CON1, CON2 with network equipment - such as, ~~for example~~, switching equipment MSC, MSC' and authentication equipment AC, AC' - is mainly responsible for matters of routing, of subscriber administration such as registration (subscription) of the subscribers S1, S2 as well as authentication, selection of the access network ACN, etc., and for offering services. The authentication procedures in the ~~means~~ <sup>authentication equipment</sup> AC, AC' preferably use secret keys  $k_i$  according to the known procedure of the GSM standard in order to implement the subscriber authentication for the subscriber S1 registered in the core network CON1 and for the subscriber S2 registered in the core network CON2 in parallel and independently of the access network ACN.

In the present example, the switching equipment MSC, MSC' in the core networks CON1 and CON2 are connected to the base station controller BSC of the access network ACN. The base station controller BSC enables the connection to at least one base station, to the base station BS in the present example. Such a base station BS is a radio station that is provided for coverage of a radio area - for example, of a radio cell - in order to setup, release and maintain connections from/to at least one mobile station MT that resides in its radio area via radio interface AI. The information are ~~thereby~~ contained in a radio channel RCH allocated by the base station controller BSC. The connections can be a matter of outgoing connections as well as of incoming connections. The mobile station MT in the present example is especially suited for simultaneous use by a plurality of subscribers S1 and

S2 that are attached in parallel to an internal bus (not shown) on the basis of their subscriber-specific devices SIM (subscriber identity module) and each have<sup>a</sup> respectively separate subscriber identity.

The mobile station MT comprises a memory ~~means~~ MSP, a <sup>transmitter and receiver</sup> transmission and reception ~~means~~ MSE as well as control devices MST, <sup>transmitter and receiver</sup> MST' that are connected to the memory ~~means~~ MSP and ~~transmission and reception means~~ MSE. Likewise, the base station BS comprises a memory ~~means~~ BSP, a <sup>transmitter and receiver</sup> transmission and reception ~~means~~ BSE as well as a <sup>controller</sup> control ~~means~~ BST that is connected to the memory ~~means~~ BSP and ~~transmission and reception means~~ BSE.

According to the invention, the mobile station MT ~~station-related via the transmission and reception means~~ MSE - sends a first public key PUK1-MT via the radio interface AI in parallel for all subscribers active at it and makes note of an appertaining, private key PRK1-MT that is deposited in the memory ~~means~~ MSP or in the <sup>controller</sup> control ~~means~~ MST. The base station BS employs the received, public key PUK1-MT for the encryption of the information to be subsequently sent via the radio interface AI. The deciphering of the information sent by the base station BS is thus only possible for the <sup>entity</sup> ~~means~~ that knows the appertaining private key, i.e., the mobile station MT with the key PRK1-MT. <sup>The base station</sup> It in turn sends a public PUK-BS in the reply of the base station BS in the opposite direction to the mobile station MT and makes note of the appertaining private key PRK1-BS. The memory ~~means~~ BSP or the <sup>controller</sup> control ~~means~~ BST stores the private key PRK1-BS. It is thus assured that information subsequently sent by the mobile station MT to the base station BS, <sup>which are</sup> ~~these being~~ encrypted upon employment of the public key PUK1-BS, can only in turn be deciphered by the base ~~station BS or its controller BST~~ station BS or, respectively, the control ~~means~~ BST thereof.

In order to prevent an "apparent" base station or unauthorized base station from using the public key PUK1-MT communicated from the mobile station MS for sending correctly encrypted information, <sup>✓</sup> arbitrarily or intentionally, the mobile station MT sends a second public key PUK2-MT (already encrypted) to the base station BS via the radio interface AI. This

key PUK2-MT can only be read and employed by the correct base station BS with which a trusted relationship was initially set up on the mobile station level. The "apparent" base station or unauthorized base station is dependably suppressed in this <sup>method</sup> ~~method~~. The second public key PUK2-MT <sup>thus</sup> ~~thereby~~ replaces the previous, first public key PUK1-MT. The same is true <sup>in</sup> ~~of~~ the other transmission direction when the mutual transmission of the keys was initiated by the base station BS.

The encryption procedure can likewise be initiated by the base station BS, so that the <sup>transmitter and receiver</sup> ~~transmission and reception means~~ BSE sends a first public key PUK1-BS to the mobile station MT, <sup>which has</sup> ~~said first public key~~ PUK1-BS having a private key PRK1-BS allocated to it and <sup>being stored in the controller</sup> ~~being stored in the control means~~ BST or in the memory ~~means~~ BSP. The mobile station MT employs the arriving, public key PUK1-BS for encryption of the <sup>that follows it</sup> ~~following~~ information and in turn sends a public key PUK-MT to the base station BS that employs it for the encryption of the information in the opposite direction. Subsequently, the base station BS preferably sends a second public key PUK2-BS to the mobile station MT in order to be absolutely certain that an undesired base station does not mix itself into the encrypted information transmission via the radio channel or <sup>eavesdrop</sup> ~~listen to this~~. The public as well as the private keys are composed, for example, of a numerical sequence or bit sequence.

Following the encryption procedure, the mobile station MT - preferably, the <sup>subscriber identity mobile card</sup> ~~means~~ SIM provided only for the authentication, or a control means MST responsible in common for encryption and authentication - implements the authentication of the respective core network CON1, CON2, and the <sup>authentication equipment</sup> ~~means~~ AC, AC' of the core network CON1, CON2 implements the authentication of the subscriber S1, S2 on the basis of mutually transmitted, encrypted information at the subscriber level (see Fig. 3). The bidirectional authentication is thus implemented independently of the access network ACN. The authentication appended to the encryption offers maximum security since it assures that the cooperating <sup>entity</sup> ~~means~~ of the connection is in fact the <sup>entity</sup> ~~means~~ that it identified itself ~~as~~ at the beginning of the communication. This prevents the overall communication on this connection



from having been initiated by an "apparent" base station or unauthorized base station. Another advantage of the functional separation of encryption and authentication is ~~comprised thereof~~ that the subscriber identities and the information required for the authentication - for example, random number RAND, <sup>and</sup> signed response SRES according to a GSM method - can already be transmitted encrypted via the radio interface A1. Authentication procedures deviating from GSM methods can also be employed for the authentication.

A plurality of core networks <sup>the</sup> the two core networks CON1, CON2 in the present example <sup>the</sup>, even if different network types, can be connected parallel to the access network ACN. The subscribers S1, S2 simultaneously work with different SIM cards via the one mobile station MT in different core networks - in the two core networks CON1, CON2 in the present example - or, respectively, one or more subscribers S1, S2 work in a single core network, for example CON1. <sup>furthermore</sup> Further, the functional separation of <sup>the</sup> access network ACN and <sup>the</sup> core network CON1, CON2 also supports configurations <sup>in which</sup> wherein the access network ACN and the core network or networks CON1, CON2 exhibit different network operators.

In a schematic illustration, FIG. 2 shows the message flow for encryption of the information for the radio transmission between the mobile station MT and the base station BS of the access network. <sup>This</sup> The example is <sup>in</sup> thereby limited <sup>thereby</sup> thereto that the mutual exchange of the keys is initiated by the mobile station MT. The base station BS could likewise begin the exchange (also see the description for FIG. 1); the following message flow would then be executed in a corresponding way.

After the allocation of the radio channel RCH for a connection setup for communication, the mobile station MT starts the encryption in that it transmits the public key PUK1-MT in a message SEND and makes note of the appertaining, private key PRK1-MT. The encrypted transmission of the information has thus begun at the radio interface. The base station BS uses the arriving key PUK1-MT for encrypted information transmission in the opposite direction, and in turn transmits the public key PUK-BS in the message SEND. It also makes note of the private key PRK1-BS belonging

to the public key PUK-BS. The information transmitted in encrypted form - at least the public key PUK-BS in the present case - can only be deciphered by the mobile station MT with the assistance of the private key PRK1-MT that is only known to it. After the deciphering, the mobile station MT sends a second public key PUK-MT to the base station BS in a further message SEND, this base station BS deciphering the arriving information - at least the second public key PUK2-MT in the present case - with the assistance of the private key PRK1-BS that is only known to it. The second public key PUK2-MT thereby replaces the previous, first public key PUK1-MT. A trusted relationship has thus been produced between the two devices, <sup>and</sup> third parties <sup>are</sup> not <sup>being</sup> capable of penetrating <sup>into</sup> this relationship.

In a schematic illustration, FIG. 3 shows the message flow for authentication of the subscribers S1, S2 registered in different core networks and for authentication of the respective core network. Messages are <sup>and are</sup> <sup>being</sup> transmitted between the subscribers S1, S2 using the mobile station MT and the network equipment AC, AC' (authentication center) of the respective core network, <sup>of it</sup> <sup>thereof</sup>.

First, the subscriber S1 or, respectively, the mobile station MT transmits an authentication request aureq-mt via the subscriber <sup>identity mobile card</sup> <sup>specific</sup> means (SIM) for the subscriber and a subscriber identity SID <sup>on the basis</sup> <sup>of the subscriber-related SIM card</sup> in the message SEND to the <sup>authentication equipment</sup> means AC of the core network responsible for the subscriber S1. The transmission of the information <sup>takes place in</sup> <sup>format</sup> <sup>encrypted</sup> <sup>thereby ensues</sup>. In the opposite direction, the <sup>authentication equipment</sup> means AC returns an authentication reply aures-co in the message SEND to the mobile station MT that implements the authentication procedure - with, preferably, a secret key - for checking the authentication for the core network. With the authentication reply aures-co, an authentication request aureq-co is preferably simultaneously co-transmitted from the <sup>authentication equipment</sup> means AC of the core network in encrypted form and is received by the mobile station MT. In response <sup>thereto</sup>, the mobile station returns an authentication reply aures-mt in the message SEND to the <sup>authentication equipment</sup> means AC in encrypted form and subscriber-

a  
a

a  
a  
a

a

*a*

Inf

INS AG